安全小课堂第七十期【Chora的白帽子之路】

京东安全应急响应中心 2017-08-18

从2013年成立到现在，JSRC在白帽子的陪伴下已经走过了四五个春秋，在这说不长也不短的日子里，JSRC积累了一箩筐的白帽子成长故事。这些白帽子故事，有些感人，有些励志，也有些坎坷。

看上去，白帽子们的日子很美好，每个重要节日都能收到JSRC送的节日礼品，能从JSRC挖掘漏洞换取苹果三件套，一年能从JSRC兑换多达十几万的礼品卡。

但JSRC知道，每一个白帽子走到今天都不容易，知道他们的付出，知道他们的心酸，知道他们一直在努力学习。

现在开始JSRC会将白帽子故事，通过安全小课堂分享给大家。

安全小课堂第七十期，JSRC邀请了仅用了一周的时间就获得了2016年年度排名前十的Chora师傅，来和大家分享他成为白帽子的故事，和大家分享他是如何学习，如何在JSRC解锁各种成就的故事。

仅用了一周的时间就获得了2016年度排名奖励,有什么诀窍吗?

京安小妹

个人认为渗透测试考验的就是经验、思路以及耐力，经验决定你的效率，思路决定你的高低，耐力决定你是否能完成目标。
非要说有什么诀窍的话，其实就是在此之前我把自己多年的渗透测试成果化，研发了一套工具集，CDomain、CInfoscan、CMap等等，能够快速精准的定位到弱点上，节约了大量精力，提高了效率，把节约的大量精力留在耐力上，而好的思路则一般是要在自己很清醒的时候才会想到。所以连续奋战毫无收获时，最好的选择不是继续死守，那样只能是浪费时间，找到的漏洞最多也是在你经验范围内的漏洞，并且还可能遗漏大量漏洞，最好的方式时眯一会儿，睡醒后再去，那样就会事半功倍。

讲师：Chora

当初为什么会选择成为一名白帽子?

京安小妹

为了避开绿帽子而成为了一名白帽子，为了维护世界的和平。。。开玩笑啦~是因为能够通过自己的努力即能为安全建设贡献自己的一分力量，在得到认可自己的同时，自己的技术也得到了提升，同时还有相应的回报，还能交到很多基友。

讲师：Chora

白帽子提问:如何培养一个好的心态?

如果其他人找到了很多漏洞，而我一个没找到的话我会觉得是自身能力不足，更应该用时间去弥补差距。
如果找的漏洞差不多，你找的漏洞别人没发现，别人找的漏洞你也没发现，则应该意识到自己擅长的和自己不足的，再接再厉。
总之就是正面的鼓励自己（并不是找借口），也不要逃避自己的缺点（正面面对，弥补知识的不足）。

讲师：Chora

在和JSRC一起成长的过程中有什么影响深刻的事吗?

京安小妹

在和JSRC一起成长过程中完善了自己的工具集。前面讲到把自己多年的渗透测试经验成果化为一套工具，结果在运用过程中发现了很多不足以及BUG，于是就变成了边刷JSRC边增加功能边修复BUG。。。顺便边带娃边挖漏洞。

讲师：Chora

你认为学习技术主要难点有哪些？如何突破？

京安小妹

学习要知其然也知其所以然，不要只会照着做，却不知道为什么要这样做。
个人认为当你自己觉得渗透测试达到瓶颈后，不妨在回过头来深入学习一门语言，成为一个攻城狮，去了解代码、了解架构。在了解它们的同时，自己也逆向思维去思考如果是你自己来写哪些地方会最薄弱，这样在你渗透测试的时候你就能够了解到整个应用最薄弱的地方。
当你觉得渗透测试再次达到瓶颈时，个人的建议是去寻找那些非常难的目标，做长时间的高强度渗透测试，然后更深入的了解语言，如此反复循环。

讲师：Chora

能否说一下对JSRC的印象以及建议？

京安小妹

JSRC的小伙伴们都很好，JSRC也很良心。
建议的话就是希望很严重的漏洞可以有额外的现金或者京东卡奖励。另外就是兑换京东卡希望是实时的E卡，直接有卡号跟密码，不跟兑换礼物一样一个月一次，单独开来。

讲师：Chora

对白帽子以及想要成为白帽子的小伙伴有什么建议？

京安小妹

对白帽子朋友的建议就是：保重身体，放下电脑立地成佛。
对想要成为白帽子的小伙伴的建议是：首先你得有耐心，坚持完成一件事，因为需要花费常人难以承受的大量精力以及时间。

讲师：Chora

白帽子提问:一般挖京东的漏洞什么类型的比较多？

都是常规的，注入、逻辑漏洞啊之类的。

讲师：Chora

白帽子提问:那么从你挖到的京东的漏洞跟挖其他企业的漏洞做比较,京东做的好的地方有哪些?做的不是很好的地方有哪些?

个人觉得SRC难度排行的话
做的好的就是比如我发现一个注入，某程序员写的你就很难发现该程序员的写的另外系统会有同样的问题，京东内部会做漏洞扫描吧。
不足的话，个人认为就是弱口令这个问题还是比其他同等级的企业多。

讲师：Chora

白帽子提问:还有就是从你的角度来说，如果给京东做安全防护，你会考虑做哪些通用一点的防护呢?

1.WAF要保证部署到每一台上线的设备，测试服跟生产服不要使用外网，这样能杜绝大部分攻击。
2.另外就是流量监测，一般做监测不管是Fuzz还是探测都会有大流量产生。
3.异常流量直接报警或者封掉，能增加攻击成本吧。
4.逻辑漏洞，这个就得黑盒白盒慢慢去测试了。

讲师：Chora

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，回复“安全小课堂”或者点击阅读原文进行查看。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心

阅读原文